Product Security Advisory: AirLink - ALEOS Security Advisory

Sierra Wireless Advisory: SWI-PSA-2023-001 (link to latest version)

Date January 27, 2023

Summary

We have received a report of potential vulnerabilities in the ACEManager configuration interface of Sierra Wireless AirLink routers running ALEOS software (referred to in this bulletin as "ALEOS devices"). The findings were reported via CERT-CC as VU #166091. We have reviewed the findings and reserve two separate CVEs for the issues identified as summarized below. Please note that both of the reported vulnerabilities require access to the ACEManager interface and knowledge of the configuration password. By default ALEOS devices ship with unique random credentials and ACEManager access is only enabled via local interfaces. For advice on how to maintain a strong security posture for your ALEOS device, please contact Sierra Wireless support personnel using the information provided at the end of this bulletin.

CVE ID	Description	CVSSv3.1
CVE-2022-46649	ACEManager iplogging.cgi remote code execution vulnerability	8.0: CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVE-2022-46650	ACEManager information exposure vulnerability	4.5: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N

Affected Products

These 2 vulnerabilties affect all AirLink routers running ALEOS software releases prior to and including version 4.9.7 (ES450, GX450) and prior to 4.16.0 (MP70, RV50, RV50x, RV55, LX40, LX60).

Scope of Impact

CVE-2022-46649: A user with valid ACEManager credentials and access to the ACEManager interface can manipulate the IP logging operation to execute arbitrary shell commands on the device.

CVSS v3.1 score: 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

CVE-2022-46650: A user with valid ACEManager credentials and access to the ACEManager interface can reconfigure the device to expose the ACEManager credentials on the pre-login status page.

CVSS v3.1 score: 4.5 (AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:N/A:N)

Recommended Actions

Upgrade to ALEOS 4.16.0 (MP70, RV50, RV50x, RV55, LX40, LX60) as soon as possible or ALEOS 4.9.8 (ES450, GX450) as soon as they are available. Pending upgrade, the following mitigations are recommended:

1. Always use strong, and ideally unique random credentials for your devices. ALEOS devices ship by default with unique random credentials.
2. Disable access to ACEManager on the WAN and make use of the Sierra Wireless Airlink Management System (ALMS) or an alternative device management platform for remote management of your ALEOS devices.
3. If you must leave ACEManager accessible via the WAN, restrict access using measures such as Private APN, VPN, or the ALEOS Trusted IP feature that restricts access to specific hosts.

Credit

Sierra Wireless would like to thank Roni Gavrilov and Eran Jacob, security researchers from OTORIO for bringing these issues to our attention. We encourage anyone with a security concern related to Sierra Wireless products to please contact us at security@sierrawireless.com.

Support Contact Information

Sierra Wireless Technical Support is available by phone or web portal from 6:00 to 17:00 PST, Monday to Friday.

Phone (Toll-Free): 1-877-687-7795
Web: https://www.sierrawireless.com/support/community-portal/

Security Bulletins

To see the latest security updates from Sierra Wireless, please visit:
https://www.sierrawireless.com/company/security/